

1 The opinion in support of the decision being entered today was *not* written
2 for publication and is *not* binding precedent of the Board.

3
4 UNITED STATES PATENT AND TRADEMARK OFFICE

5
6
7 BEFORE THE BOARD OF PATENT APPEALS
8 AND INTERFERENCES

9
10
11 *Ex parte* CAROLYN RAMSEY CATAN

12
13
14 Appeal 2007-0820
15 Application 09/734,808
16 Technology Center 1700

17
18
19 Decided: July 3, 2007

20
21
22 Before MICHAEL R. FLEMING, *Chief Administrative Patent Judge*,
23 HUBERT C. LORIN, ALLEN R. MacDONALD, LINDA E. HORNER, and
24 ANTON W. FETTING, *Administrative Patent Judges*.

25
26 PER CURIAM

27
28
29 DECISION ON APPEAL

30
31
32 STATEMENT OF THE CASE

33
34 The appeal is from a decision of the Examiner rejecting claims 5-11
35 and 13-16¹. 35 U.S.C. § 134 (2002). We have jurisdiction under 35 U.S.C.
36 § 6(b) (2002).

¹ Claims 1-4, 12, and 17 have been canceled.

1 Claims 5-11 and 13-16 are rejected under 35 U.S.C. § 103(a) (2002)
2 over Nakano (US Patent 5,845,260) in view of Dethloff (US Patent
3 4,837,422) and Harada (US Patent 5,721,583).

4 We AFFIRM.

5 Appellant's claimed invention is a consumer electronics device using
6 bioauthentication to authorize sub-users of an authorized credit account to
7 place orders over a communication network up to a pre-set maximum sub-
8 credit limit. The device includes a bioauthentication device, such as a
9 fingerprint sensor (claim 6) or voice sensor (claim 8). The claimed
10 electronics device comprises a memory, a processor, and a communications
11 link. The memory stores account information for an account holder as well
12 as bioauthentication information and sub-credit limits for authorized users
13 of the account. The processor (a) detects a match between bioauthentication
14 information received from the bioauthentication device and
15 bioauthentication information stored in memory, and when a match is
16 detected, (b) finds a sub-credit limit associated with the bioauthentication
17 information, and when a sub-credit limit is not exceeded, (c) sends account
18 holder information over the communication link to enable the user of the
19 electronics device to place an order.

20 Appellant, in the Brief², argues claims 5-11 and 13-16 as a group.
21 The Board selects representative claim 5 to decide the appeal. 37 C.F.R.
22 § 41.37(c)(1)(vii) (2006). Accordingly, the remaining claims stand or fall
23 with claim 5.

² Our decision will make reference to Appellant's Appeal Brief ("Appeal Br.," filed Aug. 9, 2006), the Examiner's Answer ("Answer," mailed Aug. 17, 2006), and to the Reply Brief ("Reply Br.," filed Oct. 17, 2006).

Claim 5 reads as follows:

5. A consumer electronics device, comprising
a memory which stores account information for an account
holder and sub-credit limits and bioauthentication information for
authorized users of the account;
a bioauthentication device which provides bioauthentication
information to the memory;
a communication link; and
a processor, which compares received bioauthentication
information to stored bioauthentication information to detect a match,
and finds an associated sub-credit limit corresponding to the received
bioauthentication information, to enable a purchase over the response
network via the communication network up to a maximum of the sub-
credit limit, the processor sending the account holder information
over the communication link only if the match is detected and the
sub-credit limit is not exceeded.

ISSUE

The issue is whether Appellant has shown that the Examiner erred in
holding the combination of Nakano's consumer electronics device and
Dethloff's and Harada's bioauthentication means would have rendered the
subject matter of claim 5 obvious to one of ordinary skill in the art at the
time of the invention.

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a
preponderance of the evidence.

1. Claim 5 does not describe the "consumer electronics device" of
the preamble in terms that limit any function, including the

steps of bioauthenticating and determining whether a sub-credit limit is exceeded, to a “local” processor.

2. The words “local” or “locally” appear nowhere in the claim.

3. According to the claim, the “consumer electronics device” *comprises* a “processor,” but the claim does not state where the processor is located or where its functions must be performed.

4. Although a “consumer electronics device” may be a single, unitary object, housing all the functions needed to operate the device, that is not always the case. Consumer electronics devices packaged to include, for example, a combination of a base station and a remote transmitter, whereby the base station processes information received from the remote transmitter (e.g., by wireless communication), are also well known.

5. Claim 5 is worded broadly and thus does not exclude such a combination.

6. Furthermore, the Specification describes, as an embodiment of the inventive device, a system wherein the bioauthentication and sub-credit limit matching functions reside on a server:

It is another object of the invention to provide a method and device, which, based on authentication of the user, enables the owner of the account to easily delegate different monetary degrees of access to the owner’s single account to different people and enables the entire family to access the account via a bioauthentication sensor. In this embodiment the account and bioauthentication information is stored at a server so that access to the server can be

1 achieved at home, at school, in a hotel, or
2 other remote location.

3 (Specification 2:20-3:4.)

- 4 7. The Specification further describes using the server as the
5 processor:

6 An authorized user then uses his PC,
7 mobile phone or television 10 to access the
8 Internet and an on-line store 11. The
9 authorized user selects an item or service for
10 purchase. The on-line store 11 requests a
11 credit card number. The bioauthentication
12 information (fingerprint, iris scan etc.) is
13 sent to the server 12. The server 12 locates
14 the correct credit card information and
15 checks whether the authorized user can
16 spend the amount requested. In one
17 embodiment, the authorized user informs
18 the server 12 of the amount to be spent and
19 in another embodiment the on-line store 11
20 gives the amount to the server. If
21 authorization is approved, the server 12
22 sends the on-line store 11 the credit card
23 information required to complete the sale.

24 (Specification 6:3-13.)

- 25 8. Because the scope of claim 5 is not limited to use of a “local”
26 processor, Nakano discloses all of the elements of claim 5
27 except for Nakano’s authentication information is not provided
28 by a bioauthentication device (Answer 3-5) (Appeal Br. 8-9).
- 29 9. The Examiner found that Harada discloses “bio-authentication
30 information as the identification information where [the]
31 bio-authentication device provides the bio-authentication
32 information that is a fingerprint (col 7, lines 19-23) further

1 where the sensor is on the remote control (col 7, lines 14-18)”
2 (Answer 6). Appellant did not traverse these findings by the
3 Examiner as to the scope and content of Harada (Appeal Br.
4 10-11 and 17-18). Thus, Harada shows that the use of a
5 bioauthentication device (fingerprint sensor) on a consumer
6 electronics device (remote control) to provide bioauthentication
7 information (fingerprint) was known in the prior art at the time
8 of the invention.

9 10. Harada teaches to use bioauthentication information, such as a
10 voice print or fingerprint, “to prevent unauthorized tampering
11 with [certain terminal setting] data by persons who may have
12 access to the remote control apparatus” (Harada, col. 4, ll. 32-
13 34), “to ensure that the type of service which is provided by a
14 terminal apparatus to the users of its remote control apparatuses
15 is selectively controlled in accordance with various different
16 categories of uses, e.g.[,] adults and children” (Harada, col. 4,
17 ll. 56-60), and “to reliably ensure that certain services which
18 should be available only to a specific individual user ... and
19 which can be requested by operation of a remote control
20 apparatus, will in fact be made available only to the appropriate
21 individual, when a number of different individuals can use
22 remote control apparatus to communicate with that same
23 terminal apparatus” (Harada, col. 4, l. 61 – col. 5, l. 3).

24 11. What is clear from Harada is that the use of a PIN code is not
25 as reliable an identifier as bioauthentication information
26 because the PIN can be stolen and used without the authorized

1 user's knowledge by anyone who may have access to the
2 remote control apparatus.

3 12. Harada suggests that bioauthentication information, such as a
4 fingerprint, unambiguously and reliably ensures that a specific
5 authorized user is requesting the service.

6 13. We further note that use of a PIN code as an identifier is not as
7 desirable as bioauthentication information because the use of a
8 PIN requires the user to remember the PIN code.

9 14. Dethloff is directed to "plastic devices, comprising integrated
10 circuits, commonly called 'smart cards'" (Dethloff, col. 1,
11 ll. 12-18).

12 15. Dethloff is specifically directed to modules or "M-cards" which
13 comprise a keyboard for entering, for example, identification
14 and transaction data, a memory for storing data, a logic means,
15 and a display (Dethloff, col. 9, ll. 57-68).

16 16. Dethloff's M-card contains means to assign the card to a
17 number of sub-users (Dethloff, col. 5, ll. 19-20), each of which
18 can be designated a particular value (Dethloff, col. 5, ll. 20-28).
19 This is accomplished by the card-holder assigning each sub-
20 user a PIN and a transaction limit (see, e.g., Dethloff, col. 6, ll.
21 64- col. 7, l. 4; Fig. 9), which are stored in a memory means in
22 the card (PIN: Dethloff, col. 11, l. 10; transaction limit:
23 Dethloff, col. 13, ll. 17-21).

24 17. In operation, a sub-user will authenticate the M-card by
25 inputting a PIN which the card then internally checks for
26 correctness (Dethloff, col. 10, ll. 63-67; see also col. 13, ll. 35-

1 38). This then triggers a means within the card to open a
2 transaction account assigned to the sub-user (Dethloff, col. 12,
3 ll. 62-64) permitting the sub-user to conduct transactions up to
4 the maximum sub-user transaction amount (Dethloff, col. 13, ll.
5 19-21).

6 18. Dethloff states that instead of a PIN, a voice print (a type of
7 bioauthentication) may be used as the sub-user enabling code:

8 It is noted that while the PIN is given
9 as an example of cardholder and sub-user
10 enabling code, any other code can be used,
11 such as a voice print (to be stored as data
12 and input by the cardholder or sub-user) . . .

13 (Dethloff, col. 11, ll. 26-29.) Thus, Dethloff explicitly shows
14 that the substitution of alternative user authentication
15 techniques is known in the prior art. In particular, Dethloff
16 teaches that it was known in the art at the time of the invention
17 to substitute a PIN authentication with bioauthentication to
18 enable a user to access credit.

19 19. The art of consumer electronics devices evidences a common
20 usage of personal codes or personal identification numbers
21 (PINs) to identify or authenticate users (e.g., Nakano, col. 4,
22 ll. 42-45 and col. 5, ll. 39-42 and Dethloff, col. 10, ll. 59-67).

23 20. The art further shows that one of ordinary skill in the consumer
24 electronic device art at the time of the invention would have
25 been familiar with using bioauthentication information
26 interchangeably with or in lieu of PINs to authenticate users
27 (Harada, col. 7, ll. 14-23 and Dethloff, col. 11, ll. 26-29.)

21. It is also clear from an examination of the prior art that those of ordinary skill in the consumer electronic device art at the time of the invention were familiar with the use of bioauthentication devices to obtain bioauthentication information to identify users (Harada, col. 7, ll. 14-23).

PRINCIPLES OF LAW

“Section 103 forbids issuance of a patent when ‘the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.’” *KSR Int’l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1734, 82 USPQ2d 1385, 1391 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18, 148 USPQ 459, 467 (1966). *See also KSR*, 127 S.Ct. at 1734, 82 USPQ2d at 1391 (“While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls.”) The Court in *Graham* further noted that evidence of secondary considerations, such as commercial success, long felt but unsolved needs, failure of others, etc., “might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented.” 383 U.S. at 18, 148 USPQ at 467.

1 In *KSR*, the Supreme Court emphasized “the need for caution in
2 granting a patent based on the combination of elements found in the prior
3 art,” *id.* at 1739, 82 USPQ2d at 1395, and discussed circumstances in which
4 a patent might be determined to be obvious without an explicit application
5 of the teaching, suggestion, motivation test.

6 In particular, the Supreme Court emphasized that “the principles laid
7 down in *Graham* reaffirmed the ‘functional approach’ of *Hotchkiss*, 11
8 How. 248.” *KSR*, 127 S.Ct. at 1739, 82 USPQ2d at 1395 (citing *Graham v.*
9 *John Deere Co.*, 383 U.S. 1, 12, 148 USPQ 459, 464 (1966) (emphasis
10 added)), and reaffirmed principles based on its precedent that “[t]he
11 combination of familiar elements according to known methods is likely to
12 be obvious when it does no more than yield predictable results.” *Id.* The
13 Court explained:

14 When a work is available in one field of endeavor,
15 design incentives and other market forces can
16 prompt variations of it, either in the same field or a
17 different one. If a person of ordinary skill can
18 implement a predictable variation, §103 likely bars
19 its patentability. For the same reason, if a
20 technique has been used to improve one device,
21 and a person of ordinary skill in the art would
22 recognize that it would improve similar devices in
23 the same way, using the technique is obvious
24 unless its actual application is beyond his or her
25 skill.

26 *Id.* at 1740, 82 USPQ2d at 1396. The operative question in this “functional
27 approach” is thus “whether the improvement is more than the predictable
28 use of prior art elements according to their established functions.” *Id.*

1 The Supreme Court made clear that “[f]ollowing these principles may
2 be more difficult in other cases than it is here because the claimed subject
3 matter may involve more than the simple substitution of one known element
4 for another or the mere application of a known technique to a piece of prior
5 art ready for the improvement.” *Id.* The Court explained, “[o]ften, it will be
6 necessary for a court to look to interrelated teachings of multiple patents;
7 the effects of demands known to the design community or present in the
8 marketplace; and the background knowledge possessed by a person having
9 ordinary skill in the art, all in order to determine whether there was an
10 apparent reason to combine the known elements in the fashion claimed by
11 the patent at issue.” *Id.* at 1740-41, 82 USPQ2d at 1396. The Court noted
12 that “[t]o facilitate review, this analysis should be made explicit. *Id.* (citing
13 *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006))
14 (“[R]ejections on obviousness grounds cannot be sustained by mere
15 conclusory statements; instead, there must be some articulated reasoning
16 with some rational underpinning to support the legal conclusion of
17 obviousness”). However, “the analysis need not seek out precise teachings
18 directed to the specific subject matter of the challenged claim, for a court
19 can take account of the inferences and creative steps that a person of
20 ordinary skill in the art would employ.” *Id.* at 1741, 82 USPQ2d at 1396.

21 The Supreme Court’s opinion in *United States v. Adams*, 383 U.S. 39,
22 40, 148 USPQ 479, 480 (1966) is illustrative of the “functional approach” to
23 be taken in cases where the claimed invention is a prior art structure altered
24 by substituting one element in the structure for another known element.
25 *KSR*, 127 S.Ct. at 1734, 82 USPQ2d at 1391. “The Court [in *Adams*]
26 recognized that when a patent claims a structure already known in the prior

1 art that is altered by the mere substitution of one element for another known
2 in the field, the combination must do more than yield a predictable result.
3 383 U.S., at 50-51.” *Id.* Ultimately the *Adams* Court found the combination
4 at issue *not* obvious to those skilled in the art because, although the
5 elements were known in the prior art, they worked together in an *unexpected*
6 manner.

7 The [*Adams*] Court relied upon the corollary principle that when the
8 prior art teaches away from combining certain known elements,
9 discovery of a successful means of combining them is more likely to
10 be nonobvious. *Id.*, at 51-52, 86 S.Ct. 708. When Adams designed
11 his battery, the prior art warned that risks were involved in using the
12 types of electrodes he employed. *The fact that the elements worked*
13 *together in an unexpected and fruitful manner supported the*
14 *conclusion that Adams’s design was not obvious to those skilled in*
15 *the art.*

16 *KSR*, 127 S.Ct. at 1740, 82 USPQ2d at 1395 (emphasis added).

17 The Federal Circuit recently concluded that it would have been
18 obvious to combine (1) a mechanical device for actuating a phonograph to
19 play back sounds associated with a letter in a word on a puzzle piece with
20 (2) an electronic, processor-driven device capable of playing the sound
21 associated with a first letter of a word in a book. *Leapfrog Ent., Inc. v.*
22 *Fisher-Price, Inc.*, 485 F.3d 1157, 1161, 82 USPQ2d 1687, 1690-91 (Fed.
23 Cir. 2007) (“[a]ccommodating a prior art mechanical device that
24 accomplishes [a desired] goal to modern electronics would have been
25 reasonably obvious to one of ordinary skill in designing children’s learning
26 devices”). In reaching that conclusion, the Federal Circuit recognized that
27 “[a]n obviousness determine is not the result of a rigid formula
28 disassociated from the consideration of the facts of a case. Indeed, the

1 common sense of those skilled in the art demonstrates why some
2 combinations would have been obvious where others would not.” *Id.* at
3 1161, 82 USPQ2d at 1687 (citing *KSR*, 127 S.Ct. 1727, 1739, 82 USPQ2d
4 1385, 1395 (2007) (“The combination of familiar elements according to
5 known methods is likely to be obvious when it does no more than yield
6 predictable results.”). The Federal Circuit relied in part on the fact that
7 Leapfrog had presented no evidence that the inclusion of a reader in the
8 combined device was “uniquely challenging or difficult for one of ordinary
9 skill in the art” or “represented an unobvious step over the prior art.” *Id.*
10 (citing *KSR*, 127 S.Ct. at 1740-41, 82 USPQ2d at 1396).

11 The person of ordinary skill in the art is a hypothetical person who is
12 presumed to know the relevant prior art. *Custom Accessories, Inc. v.*
13 *Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962, 1 USPQ2d 1196, 1201 (Fed.
14 Cir. 1986). In determining this skill level, the court may consider various
15 factors including “type of problems encountered in the art; prior art
16 solutions to those problems; rapidity with which innovations are made;
17 sophistication of the technology; and educational level of active workers in
18 the field.” *Id.* (cited in *In re GPAC*, 57 F.3d 1573, 1579, 35 USPQ2d 1116,
19 1121 (Fed. Cir. 1995)). In a given case, every factor may not be present,
20 and one or more factors may predominate. *Id.* at 962-63, 1 USPQ2d at
21 1201.

22 23 ANALYSIS

24 *Claim Interpretation*

25 Appellant argues that claim 5 should be limited to a “local” processor.
26 Claims are given their broadest reasonable construction “in light of the

1 specification as it would be interpreted by one of ordinary skill in the art.”
2 *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364, 70 USPQ2d 1827,
3 1830 (Fed. Cir. 2004). Claim 5 does not describe the device in terms that
4 limit any function, including the steps of bioauthenticating and determining
5 whether a sub-credit limit is exceeded, to a “local” processor (FF 1). In fact,
6 the words “local” or “locally” appear nowhere in the claim (FF 2). The only
7 recitation in the claim relevant to the question of where the processor and its
8 recited functions may be located in the claimed device is in the preamble,
9 i.e., in the phrase “consumer electronics device” itself. According to the
10 claim, the “consumer electronics device” *comprises* a “processor” but it
11 does not say where the processor is located or where its functions must be
12 performed (FF 3). Although a “consumer electronics device” may be a
13 single, unitary object, housing all the functions needed to operate the
14 device, that is not always the case. Consumer electronics devices packaged
15 to include, for example, a combination of a base station and a remote
16 transmitter whereby the base station processes information received from
17 the remote transmitter (e.g., by wireless communication) are also well
18 known (FF 4). The claim is worded broadly and thus does not exclude such
19 a combination (FF 5). Furthermore, the Specification describes, as an
20 embodiment of the inventive device, a system wherein the bioauthentication
21 and sub-credit limit matching functions reside on a server (FF 6, 7). In light
22 of the Specification, the claimed “device” has a broad scope and does not
23 limit the processor to one that is “locally” positioned.

24
25 *The Graham Factors*

1 The patentability of claim 5 under 35 U.S.C. § 103(a) (2002) depends
2 on whether the claimed subject matter is obvious in view of Nakano,
3 Dethloff, and Harada.

4 The Examiner found that Nakano discloses all of the elements of
5 claim 5 except for Nakano's authentication information is not provided by a
6 bioauthentication device, and Nakano fails to disclose a local storage device
7 for the memory, where the memory is part of the consumer electronics
8 device (Answer 4-5). The Appellant does not traverse these findings by the
9 Examiner (Appeal Br. 8-9). We disagree, however, with the Examiner's
10 implied finding that claim 5 requires the memory to be stored in a local
11 storage device, as discussed *supra*. Accordingly, we disagree with
12 Appellant's argument that the claimed device distinguishes over Nakano
13 because Nakano determines whether a sub-credit limit is exceeded at a
14 remote server rather than "locally." Thus, the sole difference between
15 Nakano and the subject matter of claim 5 is that Nakano does not disclose
16 the authentication information being provided by a bioauthentication device
17 (FF 8).

18 The Examiner found that Harada discloses "bio-authentication
19 information as the identification information where [the] bio-authentication
20 device provides the bio-authentication information that is a fingerprint
21 (col 7, lines 19-23) further where the sensor is on the remote control (col 7,
22 lines 14-18)" (Answer 6). Appellant did not traverse these findings by the
23 Examiner as to the scope and content of Harada (Appeal Br. 10-11 and
24 17-18). Thus, Harada shows that the use of a bioauthentication device
25 (fingerprint sensor) on a consumer electronics device (remote control) to

1 provide bioauthentication information (fingerprint) was known in the prior
2 art at the time of the invention (FF 9).

3 Because Nakano teaches every element of the device of claim 5 but
4 for the bioauthentication device element, the sole difference between
5 Appellant's claim 5 and the teachings of Nakano is the use of
6 bioauthentication in place of Nakano's password authentication (FF 8). In
7 that regard, Harada shows that it was known in the art at the time of the
8 invention to use a bioauthentication device on a remote control to provide
9 the bioauthentication information (FF 9).

10 With regard to Dethloff, the Examiner found:

11 Dethloff et al discloses bio-authentication
12 information as the identification information
13 further as a voice sensor (col 11, lines 25-30), a
14 local storage device for the memory further where
15 the memory is part of the consumer electronics
16 device (col 11, lines 2-24), sending account holder
17 information over the communication link, a match
18 detected and determining a sub-credit limit that is
19 not exceeded (col 13, lines 67-68; col 14,
20 lines 1-8).

21 (Answer 5.) We agree with the Examiner that Dethloff discloses that
22 instead of using a PIN for authentication, a voice print (a type of
23 bioauthentication) may be used as the sub-user enabling code (FF 18). As
24 such, Dethloff teaches that it was known in the art at the time of the
25 invention to substitute a PIN authentication with bioauthentication to enable
26 a user to access credit via a consumer electronics device (FF 18).

27 We find, based on our examination of the prior art and the state of the
28 art in consumer electronic devices, that the art evidences a common usage of
29 personal codes or personal identification numbers (PINs) to identify or

1 authenticate users (FF 19). The art further shows that one of ordinary skill
2 in the consumer electronic device art at the time of the invention would
3 have been familiar with using bioauthentication information
4 interchangeably with or in lieu of PINs to authenticate users (FF 20). It is
5 also clear from an examination of the prior art that those of ordinary skill in
6 the consumer electronic device art at the time of the invention would have
7 been familiar with using bioauthentication devices to obtain
8 bioauthentication information to identify users (FF 21).

9
10 *Obviousness*

11 Based on an analysis of the scope and content of Nakano and Harada,
12 the facts support the conclusion that, but for the bioauthentication means,
13 Nakano discloses all the elements of the claimed device and their functions
14 and that the bioauthentication means was disclosed in Harada. Since each
15 individual element and its function, as described in claim 5, are shown in
16 the prior art, albeit shown in separate references, the difference between the
17 claimed subject matter and that of the prior art rests not on any individual
18 element or function but in the very combination itself; that is, in the
19 substitution of Harada's bioauthentication device for Nakano's manual
20 authentication means. Where, as here "[an application] claims a structure
21 already known in the prior art that is altered by the mere substitution of one
22 element for another known in the field, the combination must do more than
23 yield a predictable result," *KSR*, 127 S.Ct. at 1740, 82 USPQ2d at 1395
24 (citing *United States v. Adams*, 383 U.S. 50-51, 148 USPQ 479, 483
25 (1966)). In that regard, Appellant has provided no evidence that replacing
26 Nakano's manual authentication means with Harada's known

1 bioauthentication means yields an unexpected result or was beyond the skill
2 of one having ordinary skill in the art.

3 The Appellant's own Specification only generally describes the idea
4 of incorporating a bioauthentication device, such as a fingerprint sensor,
5 into a consumer electronics device and the matching function needed to
6 compare the scanned bioauthentication information with the stored
7 bioauthentication information (e.g., Specification 6:6-7 and 6:17-7:2). The
8 Specification does not provide a detailed description of the implementation
9 in hardware or software of the bioauthentication device. Furthermore,
10 Appellant's Specification as well as Appellant's arguments do not present
11 any evidence that including the bioauthentication device into the consumer
12 electronic device was uniquely challenging or difficult for one of ordinary
13 skill in the art.

14 As in *Leapfrog*, the device defined by claim 5 is an adaptation of an
15 old invention (Nakano) using newer technology that is commonly available
16 and understood in the art (Harada). Adding bioauthentication to the Nakano
17 device does no more to Nakano's device than it would do if it were added to
18 any other device. The function remains the same. Predictably,
19 bioauthentication adds greater security and reliability to an authorization
20 process (FF 12). This variation on Nakano's device, whereby the manual
21 authentication means of the Nakano device is replaced with Harada's
22 bioauthentication means, appears to present no unexpected technological
23 advance in the art. One of ordinary skill in the art of consumer electronic
24 devices would have found it obvious to update the Nakano device with the
25 modern authentication components of the Harada bioauthentication means

1 and thereby gaining, predictably, the commonly understood benefits of such
2 adaptation, that is, a secure and reliable authentication procedure (FF 12).

3 Appellant argues that the Examiner has failed to provide sufficient
4 reasoning to reach a conclusion of obviousness based on the prior art
5 (Appeal Br. 11-20). Appellant repeatedly argues for application of the
6 teaching, suggestion, motivation (TSM) test, stating that “[t]here must be
7 some suggestion or motivation, either in the references themselves, or in the
8 knowledge generally available to one of ordinary skill in the art, to modify a
9 reference or to combine reference teachings” (e.g., Appeal Br. 11). The
10 Supreme Court noted in *KSR* that although the TSM test “captured a helpful
11 insight,” an obviousness analysis “need not seek out precise teachings
12 directed to the specific subject matter of the challenged claim, for a court
13 can take account of the inferences and creative steps that a person of
14 ordinary skill in the art would employ.” 127 S.Ct. at 1741, 82 USPQ2d at
15 1396.

16 The claim is to a structure already known in the prior art that is
17 altered by the mere substitution of one known element for another element
18 known in the field for the same function. The facts themselves show that
19 there is no difference between the claimed subject matter and the prior art
20 but for the combination itself. “[T]he mere existence of differences between
21 the prior art and an invention does not establish the invention's
22 nonobviousness. The gap between the prior art and respondent's system is
23 simply not so great as to render the system nonobvious to one reasonably
24 skilled in the art.” *Dann v. Johnston*, 425 U.S. 219, 230, 189 USPQ 257,
25 261 (1976) (holding that claims directed to a machine system for automatic
26 record keeping of bank checks and deposits were obvious in view of the use

1 of data processing equipment and computer programs in the banking
2 industry at the time of the invention in combination with a prior art
3 automatic data processing system using a programmed digital computer for
4 use in a large business organization). Appellant has presented no evidence
5 that combining the Nakano device with the Harada bioauthentication means
6 would have required anything more from one of ordinary skill in the art than
7 to substitute one authentication means for a more advanced one.

8 Accordingly, we hold that the subject matter of claim 5 would have been
9 obvious to one of ordinary skill in the art given the teachings of Nakano and
10 Harada.

11 Nonetheless, our holding is further buttressed by the teaching in
12 Dethoff of the substitutability of a voice print authentication for a PIN
13 authentication (FF 10). In particular, Dethloff teaches that it was known in
14 the art at the time of the invention to substitute a PIN authentication with
15 bioauthentication to enable a user to access credit (FF 10, 20).

16 Further, Harada provides sufficient motivation for one skilled in the
17 art to use this bioauthentication information, such as a voice print or
18 fingerprint, in lieu of a PIN in order “to prevent unauthorized tampering
19 with [certain terminal setting] data by persons who may have access to the
20 remote control apparatus,” “to ensure that the type of service which is
21 provided by a terminal apparatus to the users of its remote control
22 apparatuses is selectively controlled in accordance with various different
23 categories of uses, e.g.,] adults and children,” and “to reliably ensure that
24 certain services which should be available only to a specific individual user
25 ... and which can be requested by operation of a remote control apparatus,
26 will in fact be made available only to the appropriate individual, when a

1 number of different individuals can use remote control apparatus to
2 communicate with that same terminal apparatus” (FF 10). The use of a PIN
3 code is not as reliable an identifier as bioauthentication information because
4 the PIN can be stolen and used without the authorized user’s knowledge
5 (FF 11). On the contrary, bioauthentication information, such as a
6 fingerprint, unambiguously and reliably ensures that a specific authorized
7 user is requesting the service (FF12). Further, use of a PIN code as an
8 identifier is not as desirable as bioauthentication information because the
9 use of a PIN requires the user to remember the PIN code (FF 13).

10 Thus, one of ordinary skill in the art would have been motivated to
11 combine the bioauthentication device of Harada with the system of Nakano
12 because Dethloff teaches that one can substitute bioauthentication
13 information for PIN information, and Harada teaches that it was a common
14 problem at the time of the invention to create a remote control that would
15 reliably ensure that the appropriate person was given access to the system.
16 The use of a fingerprint scanner, such as disclosed in Harada, was an
17 obvious solution to provide a more reliable means of identification than the
18 PIN code of Nakano. *KSR*, 127 S.Ct. at 1742, 82 USPQ2d at 1397 (“[o]ne
19 of the ways in which a patent's subject matter can be proved obvious is by
20 noting that there existed at the time of invention a known problem for which
21 there was an obvious solution encompassed by the patent's claims.”) As
22 such, we sustain the Examiner’s rejection of claims 5-11 and 13-16 as
23 unpatentable over Nakano, Harada, and Dethloff.

24
25 CONCLUSION OF LAW

On the record before us, Appellant has failed to show that the Examiner erred in rejecting the claims over the prior art.

DECISION

The decision of the Examiner to reject of claims 5-11 and 13-16 under 35 U.S.C. § 103(a) as obvious over Nakano, Harada, and Dethloff is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

hh

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510